"Bodh", BPIT's International Journal of Technology & Management

ISSN: 2454-8421, Volume 1, Issue 1, July-Dec, 2015. *Page 89-94*

BBIJTM

Network Security Issues with ECC and El-Gamal based Threshold Cryptography

Shailendra Singh Gaur
Assistant Professor, IT, BPIT, G.G.S.I.P.U,New Delhi, India Shailendra.gaur08@gmail.com
Neha Jaitly
M.Tech, CSE, G.G.S.I.P.U, New Delhi, India n88jaitly@gmail.com
Samruddha P til
B.Tech CSE, G.G.S.I.P.U, New Delhi, India, Samruddha1401@gmail.com

ABSTRACT: ***Network security issues with EL-Gamal and ECC based Threshold Cryptography is a comparative analysis of the various cryptographic algorithms that provide efficient security to a network and guarantees delivery of data with reinforced encrypted security. A comprehensive study of these algorithms provides us with the selective information regarding their characteristics and appropriate applications. In this paper we have collaborated the encryption decryption and key generation techniques required for the operation of aforementioned cryptographic algorithms. In this paper we study diverse security issues to cloud and variety of cryptographic asymmetric key encryption algorithms adoptable to better security for the cloud & a detailed study of these encryption techniques over each other***

Keywords: ECC: Elliptic Curve Cryptography, TC: Threshold Cryptography, GMP: GNU Multiple Precision. Cloud Computing Technology (CCT)

I. INTRODUCTION

Issues in relation of network security have largely been addressed as the topmost priority whenever the installation of any network is completed. The optimal functional capabilities of network are enhanced by the employment of a security system which includes cryptographic characteristics. Elliptic Curve Cryptography (ECC) and El-Gamal cryptosystem are the most primer algorithms that can be incorporated in any network system. Further for meliorating the security of these algorithms, their integration with threshold cryptography schemes is essential. With the advent of threshold cryptography as an integral part of these algorithms the difficulty of these algorithms has increased substantially. Further this integration leads to the development of assorted algorithms such as RSA, Elliptic Curve Cryptography and El-Gamal based on Threshold Cryptography algorithms consisting of significant and critical properties which can cater extensive number of applications.

In the field of applied cryptography, Asymmetric key cryptography is most preferred because of its distinctive approach towards provision of hard to break security to various platform independent softwares. To secure the data the cryptographic algorithms are developed under the various standards which are previously set by researchers of elite internationally famed and recognized organizations and institutions.

Thus, development and application of any cryptographic algorithm is done taking the regard of these standards or the algorithms are taken as flawed and breakable. Since there has been a large number of algorithms developed by a numerous esteemed researchers with proper testing and reverse engineering, the formulation of any new algorithm to be accepted by the International standards is bound to be made keeping in mind the rules and regulations which are mandated by them. Failing to abide by the standards will not lead to the acceptance of the algorithm as it will be reverse engineered or broken

efficiently. A correct and approved algorithm only provides a system or data with the required security to protect it. [1]

II. CRYPTOGRAPHY IN NETWORK SECURITY

Network security issues are making a tremendous increase in the various dynamic, static or ad-hoc networks. These issues can be very well contained and handled by employing many cryptographic based algorithms schemes into the key generation, encryption and decryption of various sensitive data that need to be provided with efficient security. Broadly these cryptographic algorithms are classified into three sub-groups namely RSA, ECC and Threshold. The diverse domain of the network security issues pave way for the application of these algorithms with respect to the degree of security required. The comprehensive analysis and comparison of these cryptographic algorithms are essential for the determination of specific applicable algorithm to be employed to the respective network issues faced by the network.

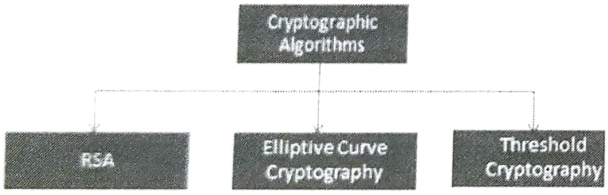

Fig 1: Classification of Cryptographic algorithms

A. Distributed Cryptography and Threshold Cryptosystems

Threshold cryptosystems are based on the alteration of the information. These alterations in the information to be transmitted are done such that it is fragmented into a number of information and distributed among bunch of collaborating computers.

The formulation of threshold cryptographic systems is such that the generation, computation and the distribution of the secret key required for the encryption and the decryption process is to be done in such a fashion that only certain number of trusted parties among all the parties is required to perform the same. This marks as a necessity for the generation of appropriate secret keys which are intended for the purpose of distribution. Advantage of such a cryptographic scheme allows the greater reliability towards the security of the data and protection from malicious party whose intent is to disrupt a significant data transaction. [2]

In order to share and distribute a secret among a category of trusted parties, there are regulations which are to be abided; the secret is carefully distributed to t+1 parties and only the honest t parties can formulate the secret. The condition is met such that no group of dishonest parties can deduce the secret even if provided with credible information about the secret itself. Here the generation of the secret can be interchanged with the generation of a message or a digital signature of the system.[3][4]

B. El-Gamal Encryption

Taher's El-Gamal proposed a cryptosystem based upon Deffie-Hellman key exchange. It incorporates an encryption scheme described over a cyclic group 'G' whose difficulty is in direct correlation with a certain problem in 'G'. In order to have a plaintext encrypted with two prime numbers say a and b which satisfies the condition a=2b+1. The cyclic group 'G' mentioned above is taken as a subgroup of $Z^*_a = \{ 1 \leq i \leq a-1 \}$. Adding to this, g will be the generator of the group. This generator g provides for the development of the public key K. Here K = (a,b,g,c) where $c = g^k \bmod a$.

The plaintext m is converted to the El-Gamal cyphertext E(m) using the combination of the public and the private key. E(m) is often represented as a pair of (g^x , mc^x) . Here the x is chosen randomly from Z^*_a. The decryption of the cyphertext E(m) is done by the computation of (mc^x / g^x). [5]

III. CLOUD COMPUTING

Cloud computing technology (CCT) is the next stage in progression of the Internet. It's a web-based computing in which huge gatherings of remote servers are organized to permit the centralized information storage, and online access to computer services or resources [6].CC is an innovation in which we can use the IT related capacity (servers, system, resources, database servers etc) on interest

basis, and pay for just utilized services not for all as we do in paying any bill according to the utilization.

The fundamental objective of CCT is to offer financially savvy, high effectiveness, dependability, adaptability, accessibility of assets, on demand access, utilization of resources over web, their online control & setup. It doesn't oblige introducing a particular bit of programming to get to or controlling cloud application. Cloud assets are accessible over the system in a way that gives autonomous access to any kind of client.[7]

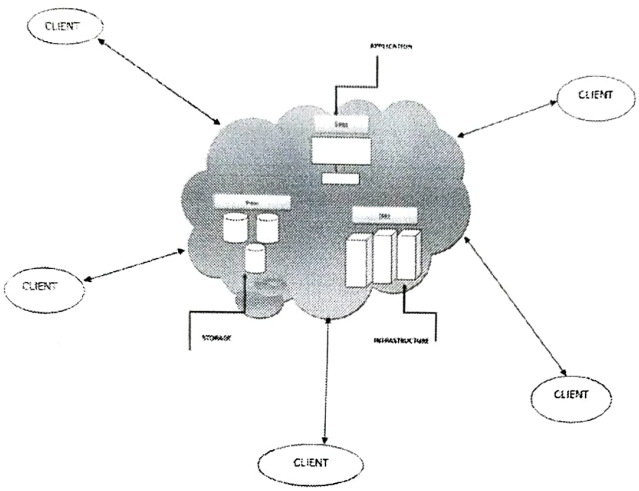

Fig.2 Basic architecture of Cloud Computing Technology

Guaranteeing the security of stored information is the most difficult issue in the cloud environment. This security has been separated to a few parts and a standout amongst the most essential parts is keeping up security in the servers of cloud computing suppliers. Hence, applying a cryptographic system for authorized client is the most famous existing answers for understanding security issues and expanding the reliability of the cloud environment.[8]

As indicated by essentialness of imparting ideas in cloud computing, Symmetric-key encryption calculations may not be suitable in these situations because of the private key offering in communication between clients. As indicated by this, Asymmetric-key (open key) cryptography calculations have been recommended by a few scientists for encoding information in cloud servers and Threshold cryptography is the most viable and prominent Asymmetric-key encryption system, when compared with others schemes that can be used for both encryption and digital signature schemes [9].

IV. GMP SOFTWARE FOR ENCRYPTION AND DECRYPTION

GNU is a free arbitrary precision arithmetic Library. It operates on signed integers, rational numbers and floating point numbers. As such, there is no particular limit to the precision except some which are imposed by the available memory we are working on. The main target applications of GMP are cryptography applications and research, Internet Security, etc.GMP uses highly optimized algorithms which results in very high speed of execution. It is designed to be as fast as possible for both small and huge operands. The speed is achieved by using full words as basic arithmetic type, also using highly optimized assembly code for the most common inner loops for a lot of CPUs.

GMP's main target platforms are Unix-type systems, such as GNU/Linux, Solaris, HP-UX, Mac OS X/Darwin, BSD, AIX, etc. It also is known to work on Windows in both 32-bit and 64-bit mode. GMP has a great set of functions which have a regular interface. The basic interface is for C but wrappers exist for other languages including Ada, C++, C#, OCaml, Perl, PHP, and Python. GMP is part of the GNU project (although its website being off gnu.org may cause confusion), and is distributed under the GNU Lesser General Public License (LGPL). GMP is used for integer arithmetic in many computer algebra systems such as Mathematics and Maple.

It is also used in the Computational Geometry Algorithms Library (CGAL) because geometry algorithms tend to 'explode' when using ordinary floating point CPU math.[10]

```
#include <stdio.h>
#include <stdlib.h>
#include <gmp.h>

int main(void)
{
 mpz_t x;
 mpz_t y;
 mpz_t result;

 mpz_init(x);
 mpz_init(y);
 mpz_init(result);

 mpz_set_str(x, "7612058254738945", 10);
 mpz_set_str(y, "9263591128439081", 10);

 mpz_mul(result, x, y);
 gmp_printf("\n"
            "     %Zd\n"
            "*\n"
            "     %Zd\n"
            "-----------------------\n"
            "%Zd\n"
            "\n", x, y, result);

 /* free used memory */
 mpz_clear(x);
 mpz_clear(y);
 mpz_clear(result);

 return EXIT_SUCCESS;
}
```

Fig 3. A program below computes the value of 7612058254738945 × 9263591128439081.

IV. CLOUD COMPUTING ISSUES IN NETWORK SECURITY

Cloud computing permits clients to accomplish the computing power not limited to their own particular physical space. Cloud computing faces generally as much security dangers that are presently found in the current stages of internet. These vulnerabilities come in different structures [11]:

Failure in cloud service provider Security: A Cloud is great when there is a decent security gave by the merchant to the clients. Supplier ought to make a decent security layer for the client and client and ought to verify that the server is generally secured from all the outer dangers it may run over.

A. Data Security Issues

Integrity: It embodies the accompanying cases, when some human blunders happen when information is entered, Lapses may happen when information is transmitted from one machine then onto another, Programming bugs or infections can likewise make infections. In this manner there is a need of some information respectability strategy in distributed computing.

- Confidentiality (Data Access Control): Some of the time private information can be illicitly accessed because of absence of secured information access control. Delicate information in a distributed computing environment develops as significant issues concerning security in a cloud based framework. Information exists for quite a while in a cloud, the higher the danger of unapproved access.
- Trust (Data theft): Distributed computing uses outer information server for cost effective and adaptable for operation. So there is a Chance of information can be stolen from the outside server.
- Availability (Data Loss/Leakage): Information misfortune loss is an intense issue in Cloud environment. Regardless of the possibility that everything is secure, imagines a scenario where a server goes down or crashes or assaulted by an infection, the entire framework would go down and conceivable information misfortune may happen. The clients won't have the capacity to get to those information's on the grounds that information is no more accessible for the client as the seller close down.

B. Hardware Related security issues:

- Hardware interruption: either as a consequence of wear-and-tear, maturity or unplanned harm.
- Hardware theft: Theft of hardware and/or information or its media
- Hardware modification: Many intruders cause change in the hardware configuration which resist the hardware to work normally [12].

C. Software related security issues:

- Insecure Application Programming Interfaces: Cloud services permit third party access by uncovering application programming interfaces; however numerous engineers and clients don't effectively secure the keys to the cloud and their data [13].
- Programming interface keys are utilized by cloud services to recognize third party applications utilizing the services. If suppliers are not watchful, an assailant with

access to the key can result in a denial of service

- Defacement: Defacement is a form of vandalism in which a website is stamped by hackers who are attempting to make their imprint.

VI. CONCLUSION AND FUTURE AREAS OF WORK

In conclusion, we address the benefits of employing an El-Gamal based Threshold Cryptographic (EG-TC) algorithm by carefully providing the implementation of the algorithm through the GMP to In order to achieve a network model which has sophisticated network security characteristics, it is important to have a structured cryptography based security protocol which lays emphasis on employment of impregnable and dynamic algorithms to counter attacks and preserve valuable data from being compromised.

A. Cryptographic Separation of Information:

All the threats have high effect on the security component of cloud computing. Here we just manage subtle element examination of data security issues of cloud computing which is Confidentiality of information for the cloud environment. The assurance of individual data or/and sensitive information, inside within cloud environment framework, constitutes a significant component for the fruitful deployment of Saas (Software as an administration) and Aaas (Application as an administration) models.

Cryptographic Separation, in which processes computations and data are concealed in such a way that they appear intangible to outsiders [14]. Confidentiality and integrity, privacy of data can be secured through encryption. Here our focus is to derive solution of cloud computing security issues "confidentiality", from asymmetric cryptography.

B. Asymmetric Cryptography for networks cloud computing provide following features:

- Authentication: The control of authenticity, identification process & exchange of information with electronic means.
- Authorization: The verified access to assets, database and informational frameworks, as per the client's consent rights and the roles.
- Confidentiality: The assurance of data either locally stored or during its transmission, from unauthorized access/users.
- Integrity: The assurance of data either locally stored or during transmission from unauthorized modification. [15]

REFRENCES

[1]. Dr.(Mrs). G.Padmavathi, Ms. B. Lavanya "Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for small Mobile Ad-hoc Networks".Int.J. Advanced Networking and Applications.Vol 03,Issue 04.2012.

[2]. Giovanni Di Crescenzo, GonazaloArce, and RenweiGe,"Threshold Cryptography in Mobile Ad Hoc networks".Security in Communication NetworksLecture Notes in Computer Science Volume 3352, 2005.

[3]. Gemmell P. S. "An Introduction to Threshold Cryptography", Cryptobytes,1997.

[4]. Adi Shamir," How to Share a Secret", Communication of the ACM, vol 22.no 11,Nov 1979

[5]. Lidong Zhou, Michael A. Marsh,Fred B. Schneider, and Anna Redz," Distributed Blinding for ElGamal Re-encryption". January 2004.

[6]. U. Somani, K. Lakhani, and M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," in Proc. 1st International Conf. on Parallel Distributed and Grid Computing (PDGC), Solan, 2010, pp. 211-216.

[7]. S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption," in Proc. 28th International Conf. of Data Engineering Workshops (ICDEW), Virginia, 2012, pp. 143-146.

[8]. Chuan Yao and Li Xu," A securecloud storage system from Threshold Encryption",5th International Conference on Intelligent Networking and Collaborative Systems, 2013

[9]. "Guide to Elliptic Curve Cryptography" By Darrel Hankerson, Scott Vanstone, Alfred J. Menezes.

[10]. The GNU MP Bignum Library". Retrieved 2013-03-17.

[11]. Pradeep Kumar Tiwari1, Dr. Bharat Mishra,"Cloud Computing Security Issues, Challenges and Solution", in 2012 International Journal of Emerging Technology and Advanced Engineering 2250-2459, Volume 2, Issue 8.

[12]. C.P. Pfleeger, S.L. Pfleeger, "Security in Computing", Prentice Hall, 2002

[13] L. H. Ying, S. S. Tzuo, T. W. Guey, and B. S. P. Lin, "Toward Data Confidentiality via Integrating Hybrid Encryption Schemes and Hadoop Distributed File System," in Proc. 26th International Conf. on Advanced Information Networking and Applications (AINA), Fukuoka, 2012, pp. 740-747.

[14]. Matthew K. Franklin, Lucas Chi KwongHui, and Duncan S. Wong , "Y. Desmedt, H. Lipmaa, and D.H. Phan. Hybrid Damg˚ard is CCA1-secure under the DDH assumption", 7th InternationalConference on Cryptology And Network Security (CANS 2008), volume 5339,2008.

[15]. Menezes .A.,Oocrchat.P., and Vanstone . S Hand book of Applied Cryptography, CRC Press 1996